PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
WILLIAM F. AHMANN
PERKINS COIE LLP
101 JEFFERSON DRIVE
MENLO PARK, CA 94025

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	08 OCT 2008
Applicant's or agent's file reference 57159-8018.WO01	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US07/20074	13 September 2007 (13.09.2007)	09 November 2006 (09.11.2006)

International Patent Classification (IPC) or both national classification and IPC

IPC: **H04L 9/00**(2006.01)
USPC: 713/175

Applicant

BROADON COMMUNICATIONS CORP.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☒ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	05 September 2008 (05.09.2008)	KAMBIZ ZAND Telephone No. (703) 305-3900

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/20074

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/20074

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay additional fees the applicant has, within the applicable time limit:
   - ☐ paid additional fees
   - ☐ paid additional fees under protest and, where applicable, the protest fee
   - ☐ paid additional fees under protest but the applicable protest fee was not paid
   - ☒ not paid additional fees
2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.
3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is
   - ☐ complied with
   - ☒ not complied with for the following reasons:

   See the lack of unity section of the International Search Report(Form PCT/ISA/210)

4. Consequently, this opinion has been established in respect of the following parts of the international application:
   - ☐ all parts.
   - ☒ the parts relating to claims Nos. 1-8 and 18-21

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US07/20074

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-8, 18-21	NO
Inventive step (IS)	Claims 1-8, 18-21	YES
	Claims 1-8, 18-21	NO
Industrial applicability (IA)	Claims 1-8, 18-21	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 18 and 20 lack an inventive step under PCT Article 33(3) as being obvious over USPub 2006/0236122 (FIELD et al), October 19, 2006 in view of USPub 2006/0153368 A1 (BEESON), July 13 2006.
As per claim 18, Field discloses a small-signature private key and a computed signature being programmed to memory of the device (Field, [0056]. Note, that the signature is generated using the small-signature algorithm using a small-signature key). Storing the private key and a computed signature in non-volatile memory is at least implicit, if not inherent. Not only Field explicitly discloses storing a small-signature private key and the signature (e.g. Field [0055-57]) but clearly these parameters should not change even after the system looses power (e.g. is rebooted) since they are used for program integrity verification each time that a program executes.
Additionally, storing data in NV memory of the device is old and well known the art of computer science and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to I use the NV memory giving the benefit of having the data accessible data after a computer is restarted.
Field discloses the use of public key but it is silent how this public key is obtained. In particular, Field does not disclose the public key being computed from the small signature private key using common parameters.
Beeson discloses computing a public key from the small-public key (Beeson, [0033]). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to compute a public key from the small-public key as disclosed by Beeson given the benefit of increased security.
As per programming a device ID and issuer ID claims these elements are found only in the nonfunctional descriptive material and it is noted that programming a device ID and issuer ID is old and well known in the art of computer science (see, e.g. service tag equivalent to an issuer ID and serial number equivalent to a device ID, for example), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include storing in NV memory disclosed by Field a device and issuer ID given the benefit of a unique identification of the device.
As per claim 20, not only Beeson discloses computing signature using an elliptic curve digital signature algorithm (DSA) (e.g. Beeson, [0021]) but also, it is noted that in the art of the cryptographic the use of elliptic curve digital signature algorithm is old and well (see Okamoto, for example). Thus, using the elliptic curve DSA would have been an obvious variation offering the benefit of security.

Claim 19 lacks an inventive step under PCT Article 33(3) as being obvious over USPub 2006/0236122 (FIELD et al), October 19, 2006 in view of USPub 2006/0153368 A1 (BEESON), July 13 2006 and further in view of Ober (USPN 6278782).
Field in view of Beeson disclose a method discussed above.
Field in view of Beeson do not disclose programming a secret seed random number in read-only memory (ROM) of the device.
Ober discloses a secret seed random number in read-only memory of the device (Ober, col. 2 lines 36-40). It would have been obvious to

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

one of ordinary skill in the art at the time of applicant's invention to program a secret seed random number in ROM as disclosed by Ober given the benefit of identifying a chip of the device.

Claims 1-3, 8 and 21 lack an inventive step under PCT Article 33(3) as being obvious over USPub 2006/0236122 (FIELD et al), October 19, 2006 in view of USPub 2006/0153368 A1 (BEESON), July 13 2006 and further in view of Giniger (USPN 6751729).
Field in view of Beeson disclose a method discussed above.
As per claim 21, Field in view of Beeson do not disclose constructing a device certificate as a function of the device ID, issuer ID, public key, signature, and common parameters.
Giniger discloses construction a device certificate providing to an application and being a function of the device ID, public key signature and common parameters (see Gininger, Fig. 5b). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include Gininger's construction of a device certificate into Field in view of Beeson's invention given the benefit of authenticating the device. Similarly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include Field in view of Beeson's invention into Giniger's invention given the benefit of ensuring integrity of applications running on the device.
Although Gininger does not disclose issuer ID being part of the certificate, including the issuer ID would not affect functionality of the certificate disclosed by Gininger and it would have been an obvious variation giving the benefit of more unique identification of the certified device.
As per claim 3, Field in view of Beeson and Giniger do not disclose the device receiving a random number and compute a signature, as a function of the random number and a private key, that is then sent via the interface. However, receinvg a random number and computing a signature as a function of the random number and private key that is sent via the interface is old and well know in the art (e.g. challenge response authentication) and it such a modification to Beeson and Giniger's invention would have been obvious giving the benefit of security.
As per claim 1, computing devices employing software communicate using interfaces (e.g. API).
Claim 8 is substantially similar to claim 20; thus, claim 8 is similarly rejected.

Claim 7 lacks an inventive step under PCT Article 33(3) as being obvious over USPub 2006/0236122 (FIELD et al), October 19, 2006 in view of Beeson (USPUB 20060/153368) and Giniger USPN (6751729), and further in view of Ober (USPN 6278782).
Claim 7 is substantially similar to claim 19; thus, claim 7 is similarly rejected.